

## **REMARKS**

Claims 1-23 are pending in the present application. By this Response, claims 1-9, 14, 15, 18-20 and 22 are amended. Claims 1, 9, 14-15, 18-19 and 22 are amended to recite that the security modification is a notification event (or the given security modification is a predetermined event) if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation. Support for this amendment is found at least on page 4, lines 3-10 and page 15, line 22, through page 17, line 4. Claims 1-2 are amended to be consistent with the amendments to claim 1 by replacing "notification event" with "predetermined event." Claim 2 is amended to incorporate the content of claims 3-4 and claim 5 is amended to incorporate the content of claims 6-8. Claims 3-4 and 6-8 are amended to claim additional features found in the specification. Support for claims 3 and 6 is found at least on page 15, line 22, through page 16, line 15. Support for claims 4 and 7 is found at least on page 4, lines 11-24. Support for claim 8 is found at least on page 8, line 19, through page 9, line 14. Reconsideration of the claims in view of the above amendments and the following remarks is respectfully requested.

### **I. Telephone Call**

Applicants thank Examiner Gurshman for the courtesies extended to Applicants' representative during the March 1, 2004 telephone call. During the call, Applicants' representative discussed the rejections to the claims and drawings. Examiner Gurshman stated that the wording of the amendments to the claims are "going in the right direction" to overcome the rejections, however he required additional time to review the reference before a final determination, as to whether the rejections were overcome, could be made. Applicants' request that Examiner Gurshman please contact Applicants' representative in the event that the rejections of the reference are not overcome. The substance of the telephone call is summarized in the following remarks.

## **II. Objection to the Drawings**

The Office Action objects to the drawings as being hand drawn figures. Applicants respectfully submit that formal drawings were filed with the United States Patent and Trademark Office (USPTO) on November 17, 2000 and a copy of the return receipt postcard indicating receipt of the formal drawings by the USPTO is attached hereto. Therefore, Applicants respectfully request withdrawal of the objection to the drawings.

## **III. 35 U.S.C. § 112, Second Paragraph**

The Office Action rejects claims 1, 9, 14, 15 and 18 under 35 U.S.C. § 112, second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention. In particular, the Office Action objects to the term "event of interest." By this Response, claims 1, 9, 14, 15 and 18 are amended to remove this phrase and thus, the rejection has been overcome. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1, 9, 14, 15 and 18 under 35 U.S.C. § 112, second paragraph.

## **IV. 35 U.S.C. § 102, Alleged Anticipation Based on *O'Toole***

The Office Action rejects claims 1, 3-8, 22, and 23 under 35 U.S.C. § 102(e) as being anticipated by *O'Toole, Jr. et al.* (U.S. Patent Number 6,279,112), hereinafter referred to as *O'Toole*. This rejection is respectfully traversed.

As to claims 1 and 22, the Office Action states:

Referring to the instant claims, O'Toole discloses control transfer of information in computer networks (see abstract and Fig. 1).

O'Toole teaches that the client computer notifies the server computer (or the information source computer) that the access ticket was added to the access control list – see column 5, lines 23-30 and Fig 2, block 32. O'Toole teaches that client computer 200 also stores a client security profile 208 that specifies that certain information in client personal profile 206 should be disclosed to server computer 202 only to trusted servers or only upon authorization from the client user or both. A client "avatar" 210 located at client computer 200 acts as an agent

for the user by controlling the release of information from client personal profile 206 to server computer 202 (see Fig. 5).

Referring to claim 1, the limitation “determining that a user has made a security modification to a portion of the trusted computing installation” is met by adding the access ticket to the access control list of the channel object of the client computer (see Fig. 1 and Fig. 2, block 30). The limitation “determining that the security modification is a notification event of interest” is met by sending the central authority a notification of the security modification” is met by client computer notifying server computer that access ticket was added to access control list (see Fig. 2, block 32).

Referring to claim 22, the limitation “a pluggable framework for receiving a set of notification objects ...” is met by notification server (see block 16 in Fig. 2).

Office Action dated December 3, 2003, page 3.

As amended, claim 1, which is representative of the other rejected independent claim 22 with regard to similarly recited subject matter, reads as follows:

1. A method for notifying a central authority of changes to a trusted computing installation, comprising the steps of:
  - determining that a user has made a security modification to a portion of the trusted computing installation under user control;
  - determining that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation;
  - and
  - sending the central authority a notification of the security modification, in response to determining that the security modification is a notification event. (emphasis added)

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicant respectfully submits that *O'Toole* does not identically show every element of the claimed

invention arranged as they are in the claims. Specifically, *O'Toole* does not teach determining that a security modification is a notification event when the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation. While the Applicants have given several examples of "circumventing" a security mechanism, e.g., allowing an unsigned applet to run or adding to or modifying the certificates in a certificate database, generally this limitation should be construed to actions which degrade the integrity of the security mechanisms of the trusted computing installation. This is not the case in *O'Toole* where a permission is merely added to the ACLs in a conventional way. Furthermore, *O'Toole* does not teach sending a notification of the security modification in response to determining that the security modification is a notification event.

*O'Toole* is directed towards methods for controlling transfers of information in computer networks, such as establishing communication channels between computers, transmitting smart digital offers based on information stored at the computer receiving the offer, automatically receiving data from a user's computer based on a personal profile and security profile of the user, and metering a user's access to linked information. One of the methods of *O'Toole* involves transmitting a document containing a channel object corresponding to a communication service from a server computer to a client computer, and storing an access ticket that indicates that a user of the client computer permits the information source computer to communicate with the user over a specified channel.

The Office Action alleges that the feature of determining that a user has made a security modification to a portion of the trusted computing installation is met by adding an access ticket to the access control list of the channel object of the client computer. The Office Action further states that the feature of "determining that the security modification is a notification event" is allegedly met by sending the access ticket to the notification server. Applicants respectfully disagree.

While *O'Toole* teaches to send the access ticket to the notification server, there is nothing in the sending of the access ticket to the notification server that teaches or even suggests that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of a trusted computing installation. To the contrary, the access ticket of *O'Toole* is the

security mechanism that provides the security necessary for the communication service from a server computer to a client computer. There is no circumvention of security mechanisms being performed by the addition of the access ticket to the access control list.

In the rejection of claim 1, the Office Action alleges that the features of claim 1 are taught by *O'Toole* at column 5, lines 23-30 which reads as follows:

Once the channel object has been activated, the client computer notifies the server computer (or the information source computer, or another computer) that the access ticket was added to the access control list (step 32) and the server computer (or the information source computer, or another computer) records in a persistent database the client's interest in the channel object and sends a confirmation to the client computer that the client's interest in the channel object has been recorded (step 34).

This portion of *O'Toole* only states that the client computer notifies the server computer that an access ticket was added to the access control list and the server sends a confirmation to the client. In other words, *O'Toole* is describing a system by which a client may "subscribe" to content being broadcast or multicast by an information source, and this "subscription" is provided in the form of an access ticket. The access ticket sets up the security for communication between a server computer and the client computer such that the server computer may push information to the client computer. *O'Toole* is teaching methods for transferring information in computer networks with the added security of an access ticket in an access control list. *O'Toole* is not concerned with determining whether a user has made a security modification that is indicative of an attempt to circumvent a security mechanism of a trusted computing installation. Thus, *O'Toole* does not teach determining that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of a trusted computing installation.

Furthermore, since *O'Toole* does not teach determining that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of a trusted computing installation, *O'Toole* cannot teach sending a central authority a notification of the security modification in response to determining that the security modification is a notification

event. The Office Action alleges that this feature is taught by *O'Toole* because *O'Toole* notifies the server computer when the access ticket is added to the access control list. However, this notification of the access ticket being added has nothing to do with a group of predetermined events that are indicative of an attempt to circumvent a security mechanism of a trusted computing installation and has nothing to do with sending a notification in response to a determination that a security modification is one of these predetermined events.

In view of the above, Applicants respectfully submit that *O'Toole* does not teach each and every feature of independent claims 1 and 22 as is required under 35 U.S.C. § 102(a). At least by virtue of their dependency on claims 1 and 22, *O'Toole* does not teach each and every feature of dependent claims 3-8 and 23. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1, 3-8 and 22-23 under 35 U.S.C. § 102(a).

Furthermore, while the Applicants might grant the Examiner's argument that the means of notification, or similar means are taught by *O'Toole* in the originally filed claims 5-8, what the notification represents, i.e., that the user is allowing circumvention of the security mechanisms, is not. The Applicants also respectfully point out, that contrary to the Examiner's statements with respect to claim 3, the addition of an access ticket to the access control list is not the same as adding a "certificate" in a certificate database. As is well known to those skilled in the art, these terms refer to distinctly different security mechanisms which operate in different ways.

The term "pluggable" is used to describe a framework, typically written in an object oriented language, in which different objects having different methods can be easily interchanged. In the Examiner's rejection of claim 22, he has presented no evidence that the notification server allows such pluggable objects, or that such objects are notification objects. *O'Toole* simply refers to messages, i.e. text, and an ACL list. Clarification of the Examiner's reasoning is respectfully requested.

The Applicants could find no argument in the Office Action which specifically addressed the limitations of claim 4. Therefore, the Office Action has not set forth a *prima facie* case of anticipation with regard to claim 4.

Furthermore, *O'Toole* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. Absent the Examiner pointing out some teaching or incentive to implement *O'Toole* to determine that the security modification is a predetermined event that is indicative of an attempt to circumvent a security mechanism of the trusted computing installation and then send a central authority a notification of the security modification, one of ordinary skill in the art would not be led to modify *O'Toole* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *O'Toole* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

**V. 35 U.S.C. § 103, Alleged Obviousness Based on *O'Toole* and *IBMC***

The Office Action rejects claims 9, 10-11, 13, 14, and 15-21 under 35 U.S.C. § 103(a) as being unpatentable over *O'Toole* in view of *INT BUSINESS MACHINES CORP [IBMC]* (RD 414099A), hereinafter referred to as *IBMC*. This rejection is respectfully traversed.

As to claims 9, 10-11, 13, 14 and 15-21, the Office Action states:

Referring to the instant claims, *O'Toole* discloses control transfer of information in computer networks (see abstract and Fig. 1). *O'Toole* teaches that the client computer notifies the server computer (or the information source computer) that the access ticket was added to the access control list – see column 5, lines 23-30 and Fig. 2, block 32. *O'Toole* teaches that client computer 200 also stores a client security profile 208 that specifies that certain information in client personal profile 206 should be disclosed to server computer 202 only to trusted servers or only upon authorization from the client user or both. The limitation “determining that a user has made a security modification to a portion of the trusted computing installation” is met by adding the access ticket to the access control list of the channel object of the client computer (see Fig. 1 and Fig. 2, block 30). The limitation “determining that the security modification is a notification event of interest” is met by sending the access ticket to notification server (see Fig. 2, block 30). The limitation “sending the central authority a notification of the security modification” is met by client computer notifying server computer that access ticket was added to access control list (see Fig. 2, block 32). *O'Toole*, however, does not teach or suggest the use of a security modification manager class.

Referring to the instant claims, INT BUSINESS MACHINE CORP (hereinafter IBMC) discloses a security environment for evaluating and executing Java applications (see abstract). IBMC teaches that the settings for each of the operation checks are defined by the JAVA security manager class (see page 2, basic-abstract). Therefore, at the time the invention was made it would have been obvious to one of ordinary skill in the art to determine that a security modification has been made to the computing installation of O'Toole and invoke a JAVA security manager class as taught in IBMC. One of ordinary skill in the art would have been motivated to determine that a security modification has been made to the computing installation and invoke a JAVA security manager class as taught in IBMC for defining the setting of the operation to be performed (see IBMC, page 2, basic abstract). The limitation "instantiating the security manager class" is met by parameters required for the application (see abstract).

Office Action dated December 3, 2003, page 4-6.

As amended, claim 9, which is representative of the other rejected independent claims 14-15 and 18-19 with regard to similarly recited subject matter, reads as follows:

9. A method of notifying a central authority of changes to a trusted computing installation, comprising the steps of:
- determining that a user has made a security modification to a portion of the trusted computing installation under user control;
  - invoking a security notification manager class;
  - instantiating the security manager class with an instance that determines that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation;
  - and
  - sending the central authority a notification of the security modification, in response to determining that the security modification is a notification event. (emphasis added)

Neither *O'Toole* nor *IBMC*, either alone or in combination, teach or suggest instantiating a security manager class with an instance that determines that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation. As stated previously, *O'Toole* is directed toward methods for controlled transfer of information in computer networks using access tickets and an access control list. *O'Toole* does not teach or suggest the above emphasized features, as previously discussed above.



*IBMC* also does not teach or suggest these features either. *IBMC* describes a shield type program that allows a user to create and deploy a security policy for a specific Java application. *IBMC* is only cited for disclosing a security manager class. *IBMC* does not teach or suggest instantiating a security manager class with an instance that determines that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation, as recited in claims 9, 14-15 and 18-19. As with *O'Toole*, *IBMC* has nothing to do with determining whether a security modification is an event that is indicative of an attempt to circumvent a security mechanism of a trusted computing installation.

Moreover, there is no teaching or suggestion in either of *O'Toole* or *IBMC* regarding the desirability of combining these two systems in the manner alleged by the Office Action. Both *O'Toole* and *IBMC* are directed toward very different problems. *O'Toole* changes the permissions granted in a centrally controlled ACL list while *IBMC* controls the behavior for a specific Java application. There is no teaching or suggestion in *O'Toole* to the effect that it would be desirable to controls the behavior for a specific Java application. Moreover, there is no teaching or suggestion in *IBMC* regarding the desirability to changes the permissions granted in a centrally controlled ACL list. Thus, the only teaching or suggestion to even attempt to combine *O'Toole* and *IBMC* is obtained from Applicants' own disclosure and is completely based on a hindsight reconstruction having first had benefit of the knowledge of Applicants' claimed invention and disclosure.

Thus, neither *O'Toole* nor *IBMC*, either alone or in combination, teach or suggest the feature of instantiating a security manager class with an instance that determines that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation, as recited in claims 9, 14-15 and 18-19. At least by virtue of their dependency on claims 9, 15 and 19, respectively, neither *O'Toole* nor *IBMC*, either alone or in combination, teach or suggest the features of dependent claims 10-11, 13, 16-17 and 20-21. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 9, 10-11, 13, 14 and 15-21 under 35 U.S.C. § 103(a).

In addition, with regard to claim 21, neither *O'Toole* nor *IBMC*, either alone or in combination, teach or suggest the specific feature of a given security manager class instance including at least first and second rules, wherein the first rule triggers a first notification and the second rule triggers a second notification. Neither *O'Toole* nor *IBMC* provide any mention regarding a given security manager class instance including rules that trigger notifications, let alone a first rule that triggers a first notification and a second rule that triggers a second notification. The Office Action does not specifically address this feature and thus, has not provided a prima facie case of obviousness with regard to claim 21.

**VI. 35 U.S.C. § 103, Alleged Obviousness Based on *O'Toole* and *Renaud***

The Office Action rejects claim 2 under 35 U.S.C. § 103(a) as being unpatentable over *O'Toole* in view of *Renaud et al.* (U.S. Patent Number 5,958,051), hereinafter referred to as *Renaud*. This rejection is respectfully traversed.

Since claim 2 depends from independent claim 1, the same distinctions between *O'Toole* and the invention recited in claim 1 apply to dependent claim 2. In addition, *Renaud* does not provide for the deficiencies of *O'Toole* with regard to independent claim 1. *Renaud* does not teach or suggest the feature of determining that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of a trusted computing installation, as recited in claim 1. Thus, any alleged combination of *Renaud* with *O'Toole* still would not result in the invention recited in claim 1, from which claim 2 depends.

*Renaud* is directed toward implementing digital signatures for data streams and data archives. The Office Action only cites *Renaud* for implementing digital signatures for data streams. Furthermore, *Renaud* does not provide any other teaching or suggestion that would result in the features of claim 1 being obviated. Therefore, even if *Renaud* were somehow combined with *O'Toole*, the result would not include the feature of determining that a security modification is a predetermined event in a group of predetermined events that are indicative of an attempt to circumvent a security

mechanism of a trusted computing installation. Thus, at least by virtue of its dependency on claim 1, claim 2 is distinguished over the alleged combination of *O'Toole* and *Renaud*. Accordingly, Applicants respectfully request withdrawal of the rejection of 2 under 35 U.S.C. § 103(a).

**VII. 35 U.S.C. § 103, Alleged Obviousness Based on *O'Toole*, *IBMC* and *Renaud***

The Office Action rejects claim 12 under 35 U.S.C. § 103(a) as being unpatentable over *O'Toole* in view of *IBMC* and further in view of *Renaud*. This rejection is respectfully traversed.

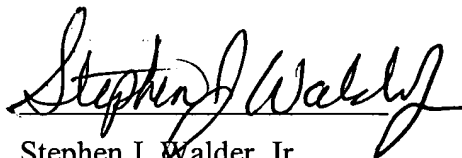
Since claim 12 depends from independent claim 9, the same distinctions between the alleged combination of *O'Toole* and *IBMC*, and the invention recited in claim 9, apply to dependent claim 12. In addition, as discussed above with regard to claim 2, *Renaud* does not provide for the deficiencies of *O'Toole*, and furthermore does not provide for the deficiencies of *IBMC*, with regard to independent claim 9. *Renaud* does not teach or suggest the feature of instantiating a security manager class with an instance that determines that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation, as recited in claim 9. Thus, any alleged combination of *Renaud* with *O'Toole* and *IBMC* still would not result in the invention recited in claim 9, from which claim 12 depends. Therefore, at least by virtue of its dependency on claim 9, claim 12 defines over the alleged combination of *O'Toole*, *IBMC* and *Renaud*. Accordingly, Applicants respectfully request withdrawal of the rejection of 12 under 35 U.S.C. § 103(a).

**VIII. Conclusion**

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: March 3, 2004



Stephen J. Walder, Jr.  
Reg. No. 41,534  
Carstens, Yee & Cahoon, LLP  
P.O. Box 802334  
Dallas, TX 75380  
(972) 367-2001  
Attorney for Applicants

Attachment:

Copy of Return Receipt Postcard  
for filing of Formal Drawings

Copy of Letter to Official Draftsman

Copy of 2 pages of formal drawings

SJW/va